Office of Attorney General Terry Goddard

STATE OF ARIZONA
DEPARTMENT OF LAW
1275 W. WASHINGTON STREET
PHOENIX, ARIZONA 85007-2926
WWW.AZAG.GOV

ANDREA M. ESQUER
PRESS SECRETARY
PHONE: (602)-542-8019
CELL PHONE: 602-725-2200

FOR IMMEDIATE RELEASE

Scam Alert: Terry Goddard Warns Consumers that Scam Artists are Phishing for Financial Data

(Phoenix, Ariz. – January 27, 2004) Arizona Attorney General Terry Goddard today warned consumers to be aware of an upsurge of e-mail scams, commonly known as "phishing" or "carding." These e-mail messages appear to be from banks, governmental agencies, financial institutions, business firms such as PayPal®, eBay® or other Internet commerce transaction sites. The e-mail messages look official because they include official-looking logos.

The e-mail will advise the recipient that something is wrong with their account, and that the victim should click on a link to "verify" personal and financial information. (Attached is an example of a phishing email sent to an employee with the Attorney General's Office).

By using the link provided inside the e-mail, the consumer will be diverted to a phony Internet Web site that appears to be an official site for the institution. An "Online Validation" form will prompt a user to enter personal or financial information: name, address, date of birth, Social Security number, driver's license number, credit card numbers and expiration dates, and PIN or security codes. Sometimes the e-mails will threaten a consumer if he or she fails to respond.

"It is important to remember that these Internet sites, no matter how authentic they look, have nothing to do with a legitimate company," Goddard said. "No legitimate financial institution will send requests for personal financial data via email."

Many times consumers are asked to download forms or other information, which could contain "Trojan Horse" programs known as spyware that allows identity thieves to invade a victim's computer, giving access to personal information stored on the computer.

Many phishers are hard to trace since they have the ability to create and dismantle a phony Web site quickly. "The key to stopping phishers is prevention, keep consumers from being conned by their schemes in the first place," Goddard stated.

Goddard offered the following consumer tips to prevent identity theft:

- If you receive a "phishing" e-mail, NEVER reply or click onto the provided link. Legitimate businesses and governmental agencies never ask for this information via e-mails.

more

- Always be cautious whenever you open any attachment or download any file from an e-mail you receive, regardless of who sends it to you. Be sure to scan emails for viruses and spyware.

- NEVER provide personally information, such as Social Security numbers, financial or bank account information, to anyone you do not already know and trust. If you are concerned over any aspect of your financial account, call the organization named in the email directly by using a telephone number that you know is genuine.

- If you believe that you may have been taken in by a phishing scam, or that you are a victim of any Internet fraud, you may contact the Internet Fraud Complaint Center (IFCC), a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Consumers can access the link and the mailing address through the Arizona Attorney General's Office at www.azag.gov.

Arizona consumers should also file a complaint online with the Arizona Attorney General's Office through the Internet by visiting www.azag.gov or contacting the Attorney General's Office by phone:

Phoenix	**Toll Free**	**Tucson**
Consumer Information & Complaints 1275 W. Washington Phoenix, AZ 85007 602.542.5763	1.800.352.8431	Consumer Information & Complaints 400 W. Congress, S-215 Tucson, AZ 85701 520.628.6504

###

Phishing Email Example:

This email was sent to a current employee at the Attorney General's Office.

Date:	Wed, 26 Jan 2005 17:12:02 +0000
From:	"Online Banking" <****@yahoo.com>
To:	XXXXXXXXXX
Subject:	Regions Bank/Bank Of The West/ People's Bank

Dear Regions Bank/Bank of the West/ People's Bank Member

This email was sent by the bank? server to verify your? email address?. You must complete this process by clicking on the link below and entering your Regions Bank/Bank of the West/ People's Bank Debit Card number and PNI that you use on ATM

This is done for your protection because some of our members no longer have access to their email address and we must verify it. To verify your email address – click on the link below:

If you have a Regions Bank savings account: http://www.regionsbank.com/?xYMkMCeV9o1JxzDn6ZqFcBuerv1x6a4j7ss6uyo2o

If you have a Bank of the West account: http://www.bankofthewest.com/?9AqmZ9efe48490LD2HbDzpAyk6w31x283

If you have a People's Bank account: http://www.peoples.com/?8CzhhZDAf0SbUoMT8If3Pauvq54c0e5916oqc9ei2b